REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** Winter 98/99	**3. REPORT TYPE AND DATES COVERED** Newsletter Vol. 2 No. 3

4. TITLE AND SUBTITLE
IA Newsletter
The Newsletter for Information Assurance Technology Professionals

5. FUNDING NUMBERS

6. AUTHOR(S)
Information Assurance Technology Analysis Center

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

A

13. ABSTRACT *(Maximum 200 Words)*

IA Newsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), Defense Information Systems Agency (DISA). This issue continues the focus on current information assurance initiatives underway within DoD, academia, and industry. In addition, an overview of current collection of Anti-Virus Tools in provided. Also featured in the issue:
OSD: JTF-CND
CINC: USACOM
Service: U.S. Army ODISC$
Systems Command: NAWCAD
R&D Perspective: Sandia National Labs
Academia: Purdue University
Industry: Harris Corporation

14. SUBJECT TERMS
Information Security, Information Assurance, Information Warfare

15. NUMBER OF PAGES
11

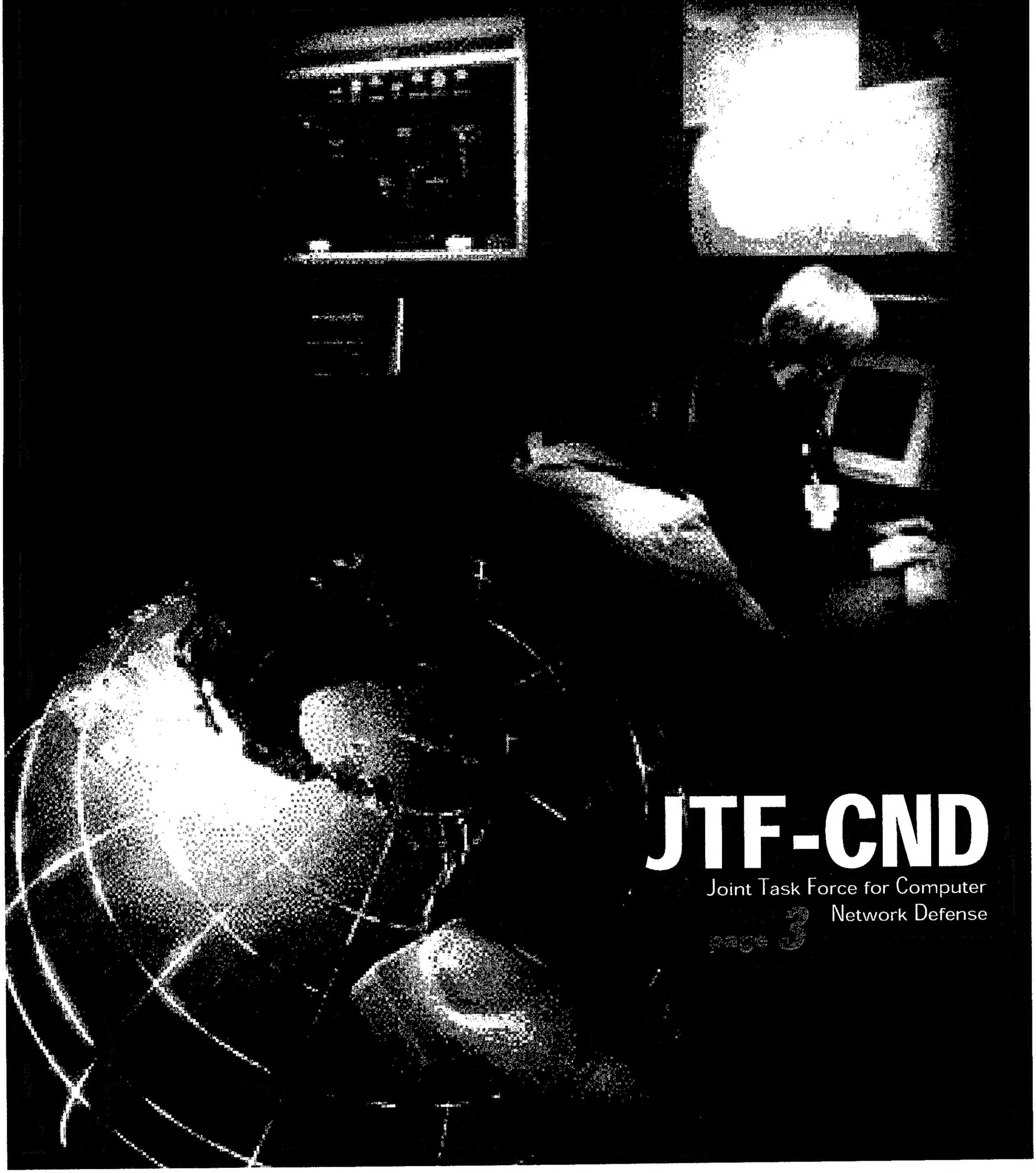
16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	None

IAnewsletter

The Newsletter for Information Assurance Technology Professionals

Winter 98/99; Vol. 2 No. 3



JTF-CND

Joint Task Force for Computer Network Defense

page 3

contents

IA Initiatives

Every Issue

IAnewsletter

Editor
Robert Thompson
Creative Director
Christina McNemar
Information Processing
Robert Weinhold
Information Collection
Alethia A. Tucker
Inquiry Services
Peggy O'Connor
Copy Editor
Kim Heanue

IANewsletter is published quarterly by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC) under the DoD IAC Program. This issue continues the focus on current information assurance initiatives underway within DoD, academia, and industry. In addition, an overview of the current collection of Anti-Virus Tools is provided.

Inquiries about IATAC capabilities, products and services may be addressed to:

Robert Thompson
Director, IATAC
703.289.5455

We welcome your input! To submit your related articles, photos, notices, feature prgrams or ideas for future issues, please contact:

IATAC
ATTN: Christina McNemar
3190 Fairview Park Drive
Falls Church, VA 22042
Phone 703.289.5454
Fax 703.289.5462
STU-III 703.289.5467

E-mail: iatac@dtic.mil
URL: www.iatac.dtic.mil

About the Cover:
The JTF-CND is collocated with DISA's Global Operations and Security Center (GOSC) in Washington, D.C.

JTF-CND

Joint Task Force for Computer Network Defense

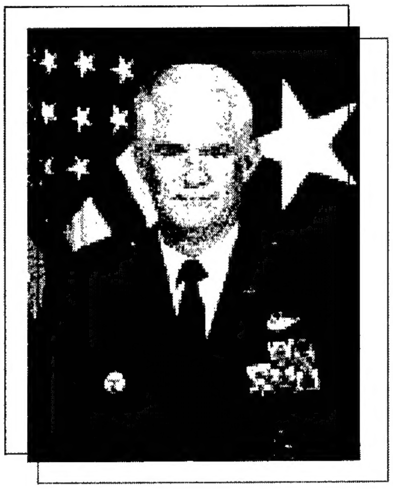
Lieutenant Colonel Robert J. Lamb
JTF-CND/D33, DISA

Information superiority— the ability to collect and process an interrupted flow of information while denying the enemy the ability to do the same, is not a new concept for the Department of Defense (DoD). The increased use of and dependence on computer technology to access and protect this information, however, is making the task of maintaining information security far more complex than before.

The DoD, like other public and private sector communities, is a computer-dependent organization. The Defense Information Infrastructure (DII) and the DoD computer networks that control and operate within it are becoming increasingly vulnerable to electronic attacks. This DoD information superhighway is becoming a "cyber battlefield" where the protection afforded by previous traditional geographical boundaries is diminished, and a threat to one DoD computer system is potentially a threat to all DoD computer systems.

Recognizing this threat, the DoD created the Joint Task Force-Computer Network Defense (JTF-CND), the first DoD organization of its kind to be the department's focal point for the defense of its computer systems and networks.

Following an extensive review of the proposed JTF-CND's location, mission, and organization, it was decided to locate the JTF-CND in Washington, D.C., with the Defense Information Systems Agency (DISA) as its supporting agency. This would allow the JTF-CND to be collocated with DISA's Global Operations and Security Center (GOSC) and to leverage DISA's existing global presence with the unified commands, its established liaisons with the law enforcement community, and its network operational view, intrusion analysis, and core technical capabilities. The JTF-CND is under the command of Air Force Maj. Gen. John H. Campbell (pictured above).



Defense Secretary William Cohen assigned the JTF-CND the following mission: "Subject to the authority, direction, and control of the SECDEF, JTF-CND will, in conjunction with the unified commands, Services, and agencies be responsible for coordinating and directing the defense of DoD computer systems and computer networks. This mission includes the coordination of DoD defensive actions with non-DoD government agencies and appropriate private organizations."

With the JTF-CND's location, command, and mission in place, the Director, Joint Staff (DJS) directed a working group be formed composed of representatives from the military services, Joint Staff, Defense agencies, and unified commands. These experts were asked to further refine the mission, help determine mission organizational functions, command relationships, budget, and manpower authorizations, and lastly, develop the concept of the operations (CONOP) for the JTF-CND.

In August the working group began meeting daily to build the JTF-CND. The group agreed to several key assumptions:

- DISA would support the JTF-CND and provide administrative, resource management, logistical, and public affairs support.
- The JTF-CND would not be a deployable asset.
- The JTF-CND would depend on intelligence community support.
- Initial operational capability (IOC) was established on 30 December 1998, requiring at least 10 personnel, and would need to fulfill 7 of the 11 mission organizational functions.
- Full operational capability (FOC) would need to be achieved no later than 6 months after IOC.

The working group's first task was to further develop the 11 mission organizational functions. Those functions included key responsibilities such as determining whether the DII was under a strategic attack, determining the impact an attack could have on military operations, coordinating and directing actions to stop, contain, and restore DoD's critical networks, and assessing the effectiveness of computer network attack restoration actions.

continued on page 4

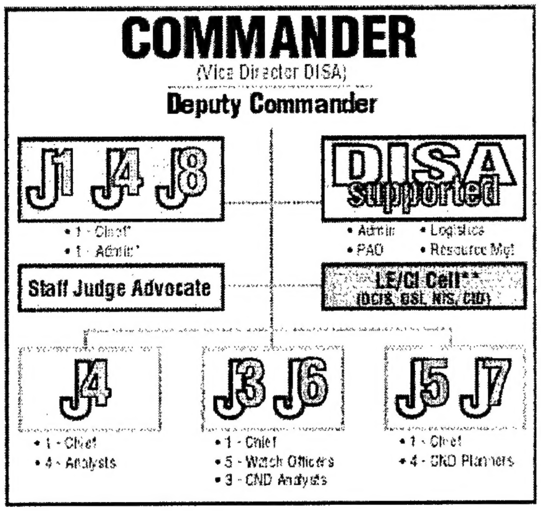


Figure 1. JTF-CND Organization

Given the JTF-CND's assumptions, mission organizational functions, and large area of responsibility (AOR), the working group then determined the organizations' personnel structure (see Figure 1). The group decided that the JTF-CND would have 24 people, which included traditional staff components. The small number of personnel assigned to the JTF-CND dictated that some of the traditional staff elements be combined (i.e., J1/J4/J8, J3/J6, and J5/J7) and that DISA employees provide administrative, resource management, logistical, and public affairs support. It was determined that the JTF-CND would also have its own Staff Judge Advocate to remain current with the laws affecting information operations, intelligence oversight, and counter-intelligence, including domestic and international laws affecting information defense options.

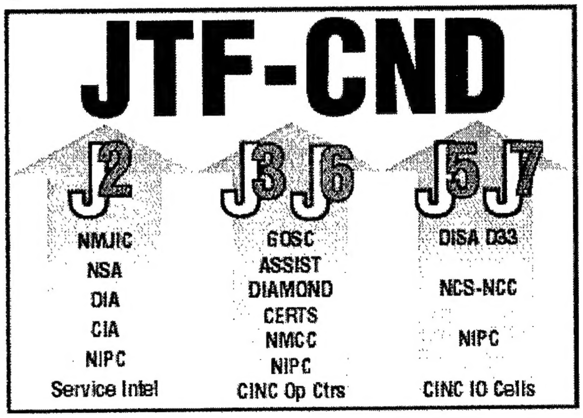
The working group's greatest challenge was defining how the JTF-CND would actually conduct its mission to coordinate and direct the computer network defense of the DII. There were several issues to consider. First, the JTF-CND had a unique DoD mission that did not correlate well to the traditional JTF structure. For example, the JTF-CND reported to the Secretary of Defense, not a commander-in-chief (CINC), and was analogous to a supporting command. Second, the AOR crossed traditional unified command and military service and agency geographical boundaries. The JTF-CND, although responsible for CND throughout the DII, would not direct a CINC how to defend that CINC's networks within his or her AOR. Third, the identification of forces (Service components) was unknown. That particular challenge extended to the Services as each grappled with selecting a force that could blend a network operation with intrusion analysis and network defense. All were available but not within the same command structure.

With these challenges identified, how will the JTF-CND execute its mission? First, the JTF-CND will leverage existing capabilities through a host of agencies and organizations, particularly the DISA GOSC and its standing relationships within the CND community. The GOSC's intrusion detection and analysis through its Automated System Security Incident Support Team (ASSIST) will serve as the immediate technical arm of the JTF-CND. The JTF-CND and the GOSC, sharing the same facility, will ensure a close working relationship and provide for the further leveraging of all technical capabilities throughout DISA. The J3 (Director of Operations) will coordinate with the National Military Command Center (NMCC) and the operation centers in the unified commands to ensure CND efforts are coordinated and synchronized with ongoing military operations. Similarly, the J5/J7 (Director for Plans and Exercises) will reach out to the commander-in-chief information operations cells and the National Coordinating Center for Telecommunications of the National Communications System to ensure planning and course of action development are conducted with a detailed view of existing operations and plans. The J2 (Director for Intelligence) will pull existing intelligence products throughout the intelligence community, including those available from the National Security Agency, the Defense Intelligence Agency, the military services, and the National Infrastructure Protection Center (NIPC).

Operating on a 24-hours, 7-days-a-week basis, the JTF-CND will fuse the operational, intelligence, and technical view of computer networks riding the DII. In turn, the JTF-CND will develop and promulgate cohesive, synchronized, and coordinated CND solutions to mitigate and defeat computer network attacks on the DII. The speed of attacks, the boundless nature of cyberspace, and the challenges of identifying the enemy demand the JTF-CND work in near real-time to accomplish its mission.

Although many questions still must be answered and new procedures established, the DoD is committed to defending its computer networks and gaining and maintaining information superiority. And today, the JTF-CND can help lead this crucial fight.

LTC Lamb received his B.S. in General Engineering from West Point and a M.S. in Education from the University of South Carolina. He is currently the Defense Information Systems Agency (DISA) liaison to the Joint Task Force for Computer Network Defense.



CPT Roderick Johnson
USACOM

Information Assurance Certification Program

At U. S. Atlantic Command (USACOM) Headquarters, the Information Assurance (IA) Branch, established in November 1997, is responsible for ensuring the availability, integrity, confidentiality, nonrepudiation, and authentication of collateral automated information systems (AIS) and the information within those systems in support of command, control, communications, and computers. As the number of Department of Defense (DoD) systems are interconnected through local and wide area networks increases,so do the opportunities for concerted attacks against USACOM AIS assets.

To protect command systems and the data they contain from being exploited, the IA Branch has developed training programs, invested in intrusion detection tools, developed security policies, and created an IA Certification Program. For a truly effective security program all these aspects of protecting computer systems must be consistently used throughout USACOM. Additionally, the cooperation of all command personnel is required to protect the integrity of shared data. To highlight one of the ways the IA Branch is maintaining USACOM's AIS security posture this article focuses on the IA Certification Program.

HOW THE IA CERTIFICATION PROGRAM WORKS

The IA Certification Program is mandatory for all assigned users and system administrators (SA) and is divided into the following three courses—

- New Users—addresses the local area network operating environment, e-mail transmissions, and various application software programs, along with physical and system security
- Security Refresher—includes current security information along with information gathered from various computer security updates.
- System Administrators—follows an intense training track involving computer-based training (CBT) modules and a skill-level checklist.

The following paragraphs overview each course.

NEW USERS COURSE

New users are required to view the DoD Information Security (INFOSEC) Awareness CBT compact disc (CD). The INFOSEC CBT CD is distributed by the Defense Information Systems Agency (DISA) and contains information on public law, information security, malicious logic, external threat methodologies and techniques, along with the individual's role and responsibility in protecting information available through computer systems.

For the New Users course, USACOM has incorporated the information contained in the INFOSEC CBT CD with an instructor-led class, certification testing, and the requirement for all new users to sign a letter acknowledging their roles and responsibilities for protecting the security of the systems to which they have been granted access. Before new users are issued a certification certificate, they must complete each part of the New Users course.

SECURITY REFRESHER COURSE.

Users who commit serious security violations (e.g., sharing passwords, misclassifying documents) are required to retake the certification test, required of all new users and described in the course above, and to attend the Security Refresher Course. Their network accounts are locked until they successfully complete the process for re-certification.

SYSTEMS ADMINISTRATORS COURSE

Various military exercises have revealed the need to ensure consistent verifiable skill sets for individuals who function as systems administrators in the system security arena. USACOM developed procedures for SA certification based on DoD Interim Guidance. For the Systems Administrators course, SAs are required to complete Operational Information System Security CBT Volumes I and II, in addition to the DOD INFOSEC CBT. The additional CBTs address several topics, including legal and regulatory issues, security incidents, trusted systems, workstation security, network security, risk management, auditing, and encryption.

Additionally, SAs, along with their supervisors, are required to complete a Job Qualification Requirements (JQR) checklist, which identifies the SA's skill level in performing necessary tasks on the USACOM systems. The checklist , in conjunction with the DoD CBTs and SA-signed letter of acknowledgement, is a key factor of USACOM's SA certification process.

USACOM's Certification Program is only the first step of many to bring security to the forefront in our information dependent environment. We must understand that it takes a coordinated effort by all to protect our information networks.

Captain Johnson received his B.S. in Computer Science from North Carolina A&T State University. He is currently the Communications Computer Systems Information Officer at USACOM in the Information Assurance Branch. His focus is training certification and policy/procedures for the Computer Intrusion Response Team. He may be reached at johnsonr@acom.mil.

Mr. Phillip Loranger
COL Michael Brown
COL John C. Deal
DISC4

Information Systems Security The New Arms Race for the Information Age

When Almon B. Strowger was an undertaker in Kansas City in 1889, he discovered a local telephone operator was compromising his funeral business. Apparently, each time prospective customers called the local telephone operator to inquire about available undertakers, the operator-who happened to be the girlfriend of Strowger's local competition in the undertaking business across town-would direct them to her friend. In response, Strowger decided to create an automatic switchboard that would eliminate all operator intervention; that is, he set out to remove human access to the control of the switch mechanism. Not only did the first "Strowger Switch" go into commercial operation in the United Kingdom in 1892, but also many remain in operation today.[1]

The key point behind Strowger's invention–to deny human access to the control of the information system–remains a critical aspect in protecting modern data networks from being compromised by hackers. Unfortunately, protecting today's data network architecture—in which control pathways are mixed with communications pathways and global systems are increasingly interconnected via the Internet—is a far more complicated task than isolating one circuit switch as Strowger did.

Modern data networks are based on information packets that are exchanged between the elements that compose the network. These various "commands" originate from both client terminals and server terminals, including packet data switches, and instruct the network when to set up a connection, tear down a connection, transfer a file, allow remote interaction, etc. The vulnerability this "open architecture" creates is a hacker need only compromise one of these commands to gain access to an information source connected to a network. When this exploitation has occurred, the entire network becomes vulnerable to further attacks.

Now consider that about 3 million computers and 20 million users compose the Internet. Daily, an increasing number of business and financial processes and services are automated. These new networks are continually placed on the World Wide Web. The current metric is that this global network of networks is doubling every 8 months. The high degree of interoperability of this burgeoning network is achieved via an established and mandated set of protocols specified by the Internet Architecture Board. The enforcement mechanism applied is simple-if you bring your network to the Internet it either complies with these protocols or it doesn't connect.

This ever-increasing reliance on data networks by the corporate world and small businesses and governmental agencies is creating an environment where organizations' data networks are becoming increasingly interconnected. This exponential growth in interconnects, in turn, creates more available pathways for hackers to exploit. Thus, the dilemma facing the corporate world, small business, and government is how to balance the openness of today's networks with security.

These opposing concepts have created an environment in which hackers are continually developing new ways to exploit data networks, while network administrators are scrambling to develop additional ways to protect these same networks. The result is a new "arms race" for weapons that will either penetrate or protect networks. The irony of conducting such a race in today's new information age is that in many cases the Web itself-with more than 30,000 sites devoted to how to exploit data networks -offers would-be hackers a wealth of easy-to-access information on attacking computer systems.

HOW HACKERS OPERATE

Hackers begin their attack by first conducting a reconnaissance of their target networks using common hacking tools such as

- WHOIS - gathers information from the InterNIC
- DNSLOOKUP - identifies associated network systems
- FINGER - identifies users and accounts
- NetScan - provides a suite of information gathering tools
- WhatsUp - provides a network mapping and monitoring utility
- Strobe - provides an automated port scanning tool.

Each of these tools is easily obtained at no cost via the various hacker Web sites. The only exception is NetScan, which costs about $30. Yet hackers can always use another tool to bypass the need for proper registration and avoid paying this fee.

After conducting their reconnaissance, hackers then exploit the network they've chosen to attack by compromising common protocols that are built into the target network itself, i.e., File Transfer Protocol (FTP), Remote Shell (RSH), and Trivial File Transfer Protocol (TFTP), in an attempt to capture the password file. The located password file is then "cracked" using a software tool such as John the Ripper-the latest password-cracking software on the market. At this point, the hacker achieves root access and super user privileges and creates a "backdoor" account into the network so the hacker can reenter the network at any time without detection. Finally, the hacker "covers his tracks" by eliminating all traces that he has manipulated the system, except for the presence of the innocuous backdoor.[2]

WHAT NETWORK ADMINISTRATORS CAN DO TO PROTECT THEIR NETWORKS

Without question the best defense against hackers exploiting known vulnerabilities in a network is for network administrators to exercise good password management. But what readily available defensive tools do network administrators have at their disposal to ensure this? Consider the following security techniques:

- To limit access, servers can contain lists of authorized users and their passwords so that to connect to the server, a client must enter an authorized UserID and password.
- To ensure UserID and passwords are not "sniffed" by hackers during the login process, Secure Socket Layer v3(SSL) can be employed. Most network and Web servers support connections over SSL, which encrypts the session from the user's Web client to the Web server. This encryption occurs before any user login or data transfer process begins. It protects the login process and the data transferred to and from the Web server. Unfortunately, the encryption algorithms used are not robust enough for classified material and can be broken by off-line processing in as little as 3 days using machines that cost as little as 250K.
- To limit access to all registered hosts and workstations in a specific Internet domain (i.e., ARMY.MIL), most Web server software has a configuration option that implements Reverse DNS Lookup. When any Internet client connects to an Internet server, the TCP/IP connection process provides the server the IP address and hostname of the Internet client. Reverse DNS Lookup takes the provided IP address and queries the domain name server to get the hostname. If the DNS lookup process is successful, it indicates that the client is a domain member (a member of ARMY.MIL) and the IP address and hostname match (a crude form of identification and authentication of the Internet client). Only if the Reverse DNS Lookup is successful, is the client allowed to access the Web server application on the Internet server.
- To further restrict access, a list of authorized IP networks or individual IP host addresses can be created. This list of allowed and denied addresses can be entered at the Web server. For UNIX machines, a TCP Wrapper or a hosts.deny list can be used. For NT Servers running Microsoft Web Server, this technique is managed through the Web software.
- To authenticate users to Web servers, user-level X.509 certificates can be used in place of UserID/passwords. These certificates provide a more scalable solution than creating individual accounts on each Web server.
- To limit who (UserID) can access a file, many operating systems allow files to have assigned Access Control Lists (ACL). If a user login is used, ACLs can further restrict access to areas on the Web server to authorized users.

Comparatively, only 1,200 sites are devoted to banking with more than 600,000 sites devoted to conspiracy theories (AXENT SWAT Team).

Forty-three percent of organizations that experienced a security breach said it cost them more than $5 million (Information Security News).

Only 55 percent of U.S. companies surveyed actively monitor network and system activity for security threats. Nearly 60 percent of those surveyed cited lack of money as an obstacle for addressing security concerns (InformationWeek/Ernst &Young).

Companies will spend more than $6.3 billion this year to bring in computer security expertise and software. Within 3 years, companies are expected to spend nearly $13 billion (Dataquest).

- To further limit who sees what on a Microsoft Web server, Microsoft offers Active Server Pages (ASP), which allows each Microsoft Web page to be dynamically created depending on who is signed on. Because this tool is for Microsoft products only, it should be used with caution and not considered a "standard" means to protect Web access.
- For Windows NT servers, user access can further be restricted to specific hours and days of the week. If this tool is enabled, specific UserIDs can access the Web server only during specific time periods.

In addition to these techniques, network administrators can build far more elaborate network security architectures. For example, Intrusion Detection Software (IDS) systems will constantly screen all Internet Protocol (IP) traffic for unauthorized entries. To achieve, this, IDS scans data traffic for pro-

MORE Hackers, Hacking & Security Threats

About 25 percent of all attacks ar e denial of service. One of the most popular hacker attacks remains "denial of service" initiatives that disrupt phone, banking, e-commerce, and other key infrastructure services but do not actually steal any electronic data.

One of the easiest ways to gain access to information is to get a job. 44 percent of computer security breaches are from unauthorized employee access to information.

The threat from outside the company has skyrocketed. 54 percent of companies report that their Internet connection is a frequent point of hacker attacks. •

Sixty-four percent of companies reported computer security breaches between March 1997 and February 1998. Seventy-two percent of these breaches caused financial losses/damages.

— Computer Security Institute

The number of Internet users rose more than 150 percent last year , with more than 130 million users already online (IDC Research). In addition, the number of remote access users will grow from more than 15 million in 1997 to more than 54 million users by the year 2002 (Gartner Group).

More than 250,000 laptop computers were reported stolen in 1996 , representing a 27 percent increase from 1995 and a loss of more than $800 million in hardware and software assets (Safeware Insurance).

Arrests for computer crimes skyrocketed 950 percent from four in fiscal 1996 to 42 in fiscal 1997. Convictions increased 88 percent from 16 to 30 (FBI reports).

files within data packets that indicate hacker activity. These packages are normally installed on a workstation connected to a device known as a security router, which routes all IP traffic to the IDS. The IDS system is installed where the private network connects to the public Internet. Firewalls, which are designed to deny entry by unauthorized users, can also be installed at network entry points or in front of a server with company sensitive information. Other evolving capabilities include public key infrastructure (PKI), which uses public and private encryption keys for all data transactions over the Internet or within an Intranet, and virtual private networks (VPN), which literally create a private network within a public network.

Overall, defensive measures can be divided into three parts-prevention, detection, and response or reaction. Prevention consists of procedural fixes such as passwords, user certification, firewalls, as well as both physical and personal security measures. For example, awareness training among a company's workforce can be highly effective in building defenses against breaches of security. Detection of intrusion can be achieved either by constantly reviewing systems logs for unauthorized activity or by installing IDS systems that can be connected to alarm and alert notification systems. Finally, responses consists of timely activities such as-

- Changing all password files
- Requiring all users to reauthenticate
- Rerouting data traffic
- Tightening IP filters and firewalls
- Enforcing certificate revocation
- Taking the system down and rebooting it
- Disconnecting a network completely from all external networks

This last response, the most extreme measure of all, works for external attacks but not internal attacks. Tracking an insider is both easy and challenging; easy because the attacker is contained and can be traced and challenging because this attacker usually possesses inside information, i.e., he or she knows the network and all its faults and traps.

THE CATCH-22 IN DEFENDING NETWORKS FROM HACKER ATTACKS

Ultimately, the same sophisticated technologies available to network administrators are also available to hackers. Consequently, as defensive measures are enhanced so are the tools of the hacker trade. The recently released "Back Orifice" by the Cult of the Dead Cows, for example, represents a significant threat to existing defensive capabilities. This tool was revealed at a hacker convention called DEFCON 6.0 from August 1 to 2, 1998. The convention is an annual gathering of about 2,500 active anarchists and hackers from around the United States and is organized by personnel of several information technology vendors, most headquartered in the Washington, DC, area. The significance of this "?BACK ORIFICE?" is that the product works effectively against all Microsoft operating systems with a version expected soon to work against Unix operating systems. It is designed to be used by people of little technical capability and can be sent to a system as a software upgrade to any Microsoft operating system. It is only 123 kilobytes in size and can be totally configured to include name and port of operation and be encrypted and appended to any application on the system. When it is attached, the infected system acts as a client to the program and full operation of the system belongs to the sending server. The only systems that cannot be affected are those that never connect to the Internet.[3]

continued on page 19

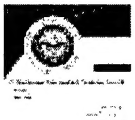
Training & Awareness Products

CD-ROM's

Operational Information Systems Security (OISS), Vol. 1

This interactive CD-ROM provides the user with an introduction to OISS, including its definition, evolution, and legal and regulatory issues associated with OISS. Topics covered include threats to Information Systems Security, examples of security violations, incident indicators and reporting procedures, Trusted Systems, and the certification and accreditation of systems. The roles and responsibilities of the ISSO, ISSM, SISSM, and SDSO are discussed. In addition, users may perform exercises at the end of each module to test their comprehension. A glossary of terms and points of contact within the INFOSEC community are provided for reference. This product is based upon the NSA course ND225, Operational Information Systems Security. 1998 EMMA Award nominee

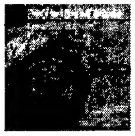
Operational Information Systems Security (OISS), Vol. 2



This interactive CD-ROM continues with OISS, including workstation, network, and storage media security, as well as encryption, malicious activity, risk management, and auditing. Topics covered include workstation and operating systems basics, network basics (including vulnerabilities, examples of violations, and security services/devices), and types/handling of storage media security. Encryption, malicious code (including the spread and detection/prevention of malicious code, with an emphasis on viruses), fundamentals of risk management, and auditing goals are also discussed. In addition, users may perform exercises at the end of each module to test their comprehension. The CD-ROM can be linked to your website for testing purposes.

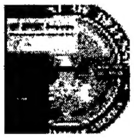
A glossary of terms and points of contact within the INFOSEC community are provided for reference. This product is based upon the NSA course ND225, Operational Information Systems Security.

DOD INFOWAR Basics



This interactive CD-ROM defines Defensive Information Warfare (IW-D) and details its evolution. Basic principles of INFOWAR are discussed as well as user roles and responsibilities. Points of contact within the Information Assurance community are provided.

DOD INFOSEC Awareness



This interactive CD-ROM explains the need for information systems security and cites recent examples of security violations. The user will learn the definition of INFOSEC, public laws relevant to INFOSEC, and government policies pertaining to INFOSEC. Other topics covered include external threats to information security, the evolution of INFOSEC, user roles and responsibilities, and malicious logic. A glossary of terms and a directory of where to find help within the INFOSEC community are provided for reference.

Federal INFOSEC A wareness

This interactive CD-ROM explains the need for information systems security and cites recent examples of security violations. This product is intended for a Federal, non-DOD audience. The user will learn the definition of INFOSEC, public laws relevant to INFOSEC, and government policies pertaining to INFOSEC. Other topics covered include external threats to information security, the evolution of INFOSEC, user roles and responsibilities, and malicious logic. A glossary of terms and points of contact within the Federal INFOSEC community are provided for reference. 1998 New Media Invision Award nominee

Introduction to the Defense Infor mation Technology Security Certification & Accreditation Process (DITSCAP)

This interactive CD-ROM provides the user with an overview of the DITSCAP, including its definition, the evolution of information systems security, and roles and responsibilities. Modules 2 through 5 cover Definition, Verification, Validation, and Post-Accreditation. All modules include an overview of topics covered, a description of process activities, and individual, team, and group roles and responsibilities.

Information Age T echnology

This interactive CD-ROM includes an overview of basic information technology infrastructures, such as the Defense Information Infrastructure (DII), National Information Infrastructure (NII), Global Information Infrastructure (GII), and Intelligence Information Infrastructure (III). Topics covered include considerations in information transportation, such as speed, throughput, security, cost, and distance. Various types of media for sending messages across the information infrastructure are also discussed. One module highlights the hardware and resources used to support the information infrastructures, with an emphasis on communication devices used to access, process, and transmit in-

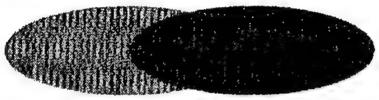
continued on page 20

Gary E. Lohman, Ph.D.
Naval Air Warfare Center Aircraft Division

Risk-Based Decision Making

Do you feel secure in your decisions? There are many descriptive and prescriptive theories for risk-based decision making. The kernel of these theories is a drive towards "security" as measured by reasonable assurances in conjunction with acceptable risks. Such security is a relative feeling or perception of "comfort" that differs among people and situations, thus giving rise to fundamentally different decision-making styles. Specifically, some decision makers take greater risks, while other decision makers seek greater assurances. Good decision makers tend to be skilled at both assessing risks and managing assurances. Based on this understanding of decision-making styles, the term "security" can be readily defined as follows:

SECURITY = "Assurance" ∩ "Certainty"



Security is a level of confidence based on both the assurance that a system can perform as required and the risk-related certainty that a system will perform as required given an inherent dynamic threat environment in which the system exists.

In short, security is the intersection of "can" and "will" as depicted by the Venn-diagram in Figure 1.

Accurate information is essential for making good decisions... Decisions are in essence conclusions drawn from information derived from the decision making processes. Data feeding into the decision processes derive from the business operations, specifically from the information in operations as well as the intelligence, and counterintelligence processes. Inherent in business operations information, for example, are the notions of quality and configuration control information along with both internal and external competitive forces and trends. Consequently, decisions resulting from such information tend to be directive in nature feeding back into the business operations through the established business processes of the particular business or organization.

The evolution of technology and the drive of competitive forces in the 20th century, however, have drastically transformed business processes, operations, and organizational structures across industrialized societies. These factors have propelled business systems along an evolutionary path of automation, federation and now integration. Integration goes beyond the automated processes, systems, and businesses across common infrastructures. Integration dictates that these components share common information across the common infrastructures to create effective value chains in product development. In this environment, information dominance and infrastructure superiority are essential foundations for conducting integrated business operations.

Well-integrated information operations (IO) provide the functional information link within business operations between the input and output of the decision process. Figure 2 depicts this information perspective of the decision process. Information assurance (IA), information warfare (IW), and information-in-operations (IIO) form the three functional groups under the IO umbrella within business operations. Further division of these functional groups depends on the specifics of a particular organization's business operations as defined through the business value chain supporting the product development cycle. Applying this to DoD would entail a detailed analysis of the coupled life-cycle acquisition, support and crisis response processes across CINC's, Services and Agencies as applied to products such as humanitarian aid, peace-keeping or peace-making and is thus outside the scope of this article.

The net effect of this development on today's decision-making process is an increased reliance on closely coupled long and short term decisions in maintaining an active business stability in an information-rich, highly changeable environment. This is in direct contrast to traditional business stability achieved by the inertia of hierarchical organizational structures and redundant processes, etc. Active stability equates to rapid and deliberate decision making based on the near-real-time coupling of information to and from the business operations. The fundamental decision process has thus not changed, but our active reliance on the process has dramatically increased within the information age and thus fueled the interest in risk-based decision making methods?.

STEADY STATE DECISION MODEL...

For every situation some minimum acceptable security based on some measure of assurance and measure of certainty (risk) exists. Figure 3 relates this concept to a heuristic minimum of acceptable security. As the figure of merit indicates, the ideal decision case is one of perfect assurance and perfect certainty; the realistic decision cases, however, tend to be within the acceptable certainty (risk) and reasonable assurance ranges. The figure of merit applies the Venn-diagram definition of security, Figure 1, as the product of assurance and certainty. Assuming these are normalized quantities, i.e., defined on the interval of 1≥x≥0, then certainty can be interpreted as the relative absence of risk or simply 1-Risk. Consequently, we obtain a rather elegant algebraic expression for security:

That is, security is defined by the assurance less that portion of assurance sacrificed through risk. Zero risk, which corresponds to a threat-free environment, implies that our security is defined simply by assurance, i.e., our confidence that the system can perform. Conversely, total risk Of unity, i.e. Risk=1, would completely sacrifice the assurance and yield zero security as one would expect. Short-term or tactical decisions are generally made in direct response to a perceived threat. The acceptable risk given a threat scenario with respect to the minimum acceptable security in light of defined assurance can thus be characterized as follows.

The degree of risk can be Characterized through a simple figure of merit, illustrated in figure 4, based on the product of impact and vulnerability. As the heuristic maximum risk acceptance curve in figure 4 suggests, high impact coupled with low vulnerability or high vulnerability coupled with low impact are both of lesser concern than a moderate impact combined with a moderate vulnerability. Because human nature tends to lead us to focus on extremes either in terms of impact or vulnerability, we usually ignore the more common moderate-moderate situations in between. Not only can these in-between situations be more disconcerting, but their underlying causal relations can result in domino effects within the middle region that further enhance the expected concavity of the risk acceptance curve in the figure of merit.

As the additional Venn-diagram in figure 4 indicates, vulnerability itself can be viewed as a compound quantity obtained from assessing potential system weaknesses weighted by the estimated probability or frequency of exploitation based on an underlying understanding of threat. Vulnerability can thus be interpreted as a weighted measure of likelihood. Impact, however, relates to the potential result of sacrificed assurances. Consequently, defining security at any point in time relies on assessing "have" and "sacrificed" assurances relative to "required" assurances. Two key sets of metrics—required assurances and applicable threats—emerge as central to making tactical decisions based on the time-slice perspective of security.

Required assurances and applicable threats are both related to the mission and vision of the respective organization. Consistently successful decision makers usually have a firm grasp of their vision in terms of goals and the critical success factors that determine how well the goals are being achieved. The point of identifying required assurances is to define the set of criteria representing both the necessary and sufficient assurances relative to the critical success factors. In this way, we focus on correctness rather than completeness. Necessary assurances for business operations include functionality, reliability, survivability, maintainability, affordability etc. Sufficiency of each of these assurances can be ensured by mapping the defined criteria to the assurance services of confidentiality, integrity, availability, accountability, etc. Based on an assurance matrix of the required criteria, assurances can be parameterized and weighted. An assessment at any point in time relative

continued on page 14

Anti-Virus

See What's New on page 22 for summary & ordering information.

NAME	COMPANY	URL
Quick Heal	Cat Computer Services	http://www.quickheal.com
Command Antivirus	Command Software Systems, Inc	http://www.commandcom.com
InoculateIT	Computer Associates	http://www.cai.com/cheyenne
V-find Security Toolkit	Cybersoft	http://www.cyber.com
Wave Anti-Virus	Cybersoft	http://www.cyber.com
F-Secure Anti-Virus	Data Fellows	http://www.datafellows.com
Adinf	Dialogue Science	http://www.dials.ru
Dr. Web	Dialogue Science	http://www.dials.ru
EMD Armor	EMD Enterprises	http://www.emdent.com
ESafe Protect Enterprise	Esafe Technologies	http://www.esafe.com
ESafe Protect Gateway	Esafe Technologies	http://www.esafe.com
NOD-iCE	ESET	www.eset.sk
AVG Anti-Virus System	Grisoft	http://www.grisoft.com
IRiS AntiVirus Plus	IRiS Antivirus	http://www.irisav.com
Antiviral Toolkit Pro	Kaspersky Labs	http://www.avp.ru
VirusBuster	Leprechaun Software	http://www.leprechaun.com.au
Virus ALERT	Look Software	http://www.look.com
PC ScanMaster for VINES	Netpro	http://www.netpro.com
Server ScanMaster for VINES & NT	Netpro	http://www.netpro.com
Dr. Solomon's Anti-Virus Toolkit	Network Associates, Inc.	http://www.nai.com
McAfee VirusScan	Network Associates, Inc.	http://www.nai.com
NetShieldNT	Network Associates, Inc.	http://www.nai.com

See What's New on page 22 for summary & ordering information.

Anti-Virus

NAME	COMPANY	URL
Invircible	NetZ Computing	http://www.invircible.com
ResQProf	NetZ Computing	http://www.invircible.com
Norman Virus Control	Norman Data Defense Systems	http://www.norman.com
ThunderBYTE	Norman Data Defense Systems	http://www.norman.com
DisQuick Diskettes	OverByte Corporation	http://www.disquick.com
Panda Antivirus	Panda Software	http://www.pandasoftware.com
Protector Plus	For Windows 95/98, Netware, and NT	http://www.pspl.com
DiskNet	Reflex Magnetics	http://www.reflex-magnetics.co.uk
MIMEsweeper	Content Technologies, Inc.	http://www.mimesweeper.com
VirusNet LAN	Safetynet	http://www.safetynet.com
VirusNet PC	Safetynet	http://www.safetynet.com
AVAST	Securenet	http://www.securenet.org
System Boot Areas Anti-Virus & Crash Recovery		SBABR http://www.sbabr.com
Sophos Sweep	Sophos Software	http://www.sophos.com
Integrity Master	Stiller Research	http://www.stiller.com
Antigen 5 for Lotus Notes	Sybari	http://www.sybari.com
Antigen 5 for Microsoft Exchange	Sybari	http://www.sybari.com
Norton Anti-Virus	Symantec Corporation	http://www.symantec.com
InDefense	Tegam, International	http://www.indefense.com
OfficeScan	Trend Micro	http://www.antivirus.com
ServerProtect	Trend Micro	http://www.antivirus.com
VET Anti-Virus	VET Anti-Virus Software Pty LTD	http://www.vet.com.au/

continued from page 11

to this matrix yields the "have," and "sacrificed" assurances with respect to the "required" assurances. In terms of the previously derived definition of security, this yields a relation of the following form.

Required assurances and applicable threats are related closely and must in practice be developed and assessed concurrently. Threat scenarios must be developed based on motives, methods, and opportunities consistent with the required assurances but also from the perspective of the threat agent. For tactical decisions made in response to a threat, it is the probabilistic "likelihood" that is crucial to the decision maker, thus yielding the following tactical decision-making figure of merit.

TIME-INTEGRATED DECISION MODEL

The deliberate decision process guarantees a decision made by a defined decision authority as opposed to a decision reached by committee. The deliberate decision process has always been an important asset of the military based on the concept that it is riskier not to make a decision (i.e., allow the decision to be made for you) than to risk making a wrong decision. The timely availability of information combined with the ability to interpret the information in terms of required assurances and probable risks are the keys to making consistent tactical decisions using the steady-state decision model. Furthermore, seldom does the outcome of a situation depend on a single decision. Consistency may not guarantee that every decision will be correct, but it will guarantee likelihood of expected outcome leveraged across the individual decisions of a common strategy. The time-slice or instantaneous notions of assurance and risk are important for individual tactical decisions, but the time-integrated perspective becomes essential for strategic decisions.

Decisions are discrete in nature. If we consider the security resulting from a typical decision as a function of time, we note that security (due to inherent uncertainty) starts out comparatively low but increases to a level at which point in time the real benefits from the decision can be harvested. Due to an inherently changing environment (decreasing assurance with increasing risk), security will tend to decrease after some point in time without re-evaluation and correction of required assurances with respect to new and evolving threats. This re-evaluation and correction of required assurances forms an important basis for strategic or long-term decisions. Strategically, it is important to make the long-term decisions before the major decrease in security occurs so as to allow a transition without a significant decrease in security prior to some "sunset" point. In this way, the tactical decisions become intimately coupled with the strategic decisions within the overall framework of the organization's vision and the evolution of an inherent threat environment. Figure 5 shows this strategic perspective by considering such long-term decisions as "investments." In terms of assurances, the "required," "have," and "sacrificed" factors are all time-dependent. Similarly, threats, and subsequently vulnerabilities, can also be expected to evolve over time. Finally, note the initial reinvestment security in figure 5 is slightly higher than the initial investment security so that the algebraic sum of the ongoing investment security with the reinvestment security at every point in time is within the minimum acceptable security level. Too early or too late reinvestment results in insecurity similar to late transitions and sunsets. The overall investment strategy must be in line with acceptable minimum security and consistent with the overarching vision.

TAKE HOME MESSAGE...

It is generally held that people both fear and dislike change. Yet, good decision makers are able to embrace change and harness its potential to their advantage. Effective and consistent decision making depends on a systemic method for interpreting assurance and risk in such a way so as to leverage tactical decisions within a strategic framework. Well-planned strategic decisions in conjunction with properly leveraged tactical decisions are the key to smooth sailing through risky waters. In the end, decision making is neither as precise as a science nor as subjective as an art form, but it is a statistically predictable skill that anyone can in principle master.

Gary Lohman is....

Rick Craft,
Sandia National Laboratoriies

Sandia Researches The Next Generation of Security Engineering Tools

Security engineering, as it is practiced today, is largely a manual process. Although software tools do exist to automate some portion of the security-engineering life cycle, none yet support the full spectrum of activities that can be performed when securing a system. In general, these tools are based on an oversimplified view of the system, assume that known vulnerabilities are the only avenues of attack open to an adversary, and tend to apply safeguards in a prescriptive fashion that fails to account for both the unique aspects of the system at hand and the hidden costs associated with selecting specific safeguards. Although these tools are useful, as far as they go, they are also dangerous if trusted blindly.

Because security engineering is a manual process, it is also time-consuming and expensive. Further, it can be an error-prone process because the quality of the process' results is often directly related to the expertise of the analysts securing the system. At the core of these problems is the reality that security engineering is still more art than science.

For these reasons, in 1996 Sandia National Laboratories began to investigate the development an open framework that would integrate all the activities associated with the engineering of secure systems. As it was conceived, this framework would support the analysis and safeguarding of multi-technology systems (not just information systems) and would allow a broad range of security engineering tools to be used in a mix and match fashion.

After studying many of the methodologies used both inside and outside the information security community, the research team formulated an approach to security engineering that unified various security engineering methods by means of an explicit system model. In this approach, the system is modeled as a collection of cooperating components. These components can represent tangible items such as computers, people, or buildings, or abstract entities, such as mission-level functions or software processes. In building the model, the analyst documents how the various components in the system being assessed influence one another and how each component reacts under various influences. Component vulnerabilities are treated as extensions to the component's behavior. Threat agents and safeguards are treated as additional system components that send, receive, or block flows in the system. Attacks are defined as the series of component interactions that connect initiating events with undesired outcomes within components or flows between components. Given the system model, analyses consist of selecting a point in the system model to investigate and then "slicing" out of the system model those parts of the model that affect the selected point (either directly or indirectly) or those parts that are affected by the selected point. The research team showed that such analysis can be done automatically with the help of software tools and can be used to support several flow-based analysis techniques (e.g., fault-tree analysis or failure modes and effects analysis).

To assess the feasibility of this security-engineering approach, the research team produced a prototype "tool kit" in 1998 based in part on the Rational ?OK Rose CASE tool. This work is continuing in the context of a source code assessment tool being developed at Sandia. By the end of FY99 the research team expects to deliver a first version of the source code assessment tool kit, which will include the ability to model the software system's context (e.g., the external, non-software devices with which the software interacts) and to assess the system and its context as a whole. The final version of this tool kit is expected to be ready by the end of FY01.

Although Sandia's research has pointed the way to the next generation of security engineering tools, the research has also highlighted several problems for which the security community currently has no good answers. Any organizations wishing to discuss the results of this research or the problems identified can contact the author at 505-844-8873 or rlcraft@sandia.gov.

Rick Craft is a senior member of the technical staff at Sandia National Laboratories, where he has worked since 1981. He holds an MS in electrical engineering and has spent the majority of his career in system analysis and software engineering. Since 1992, he has worked as a security analyst in the Information Systems Surety department and as part of Sandia's Information Design Assurance Red Team (IDART) activity.

by Sofie Nystrom
Purdue University

EDUCATING The Next Generation of Computer Security Specialists

"The public perception of computer security is shaped by sensationalism such as computer virus scares and stories of teenagers breaking into sensitive military systems," Professor Eugene Spafford, Director of the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University, Indiana states, "but information and computing security is far more complex than that and involves disciplines including sociology, psychology, criminology, political science, ethics, management, and economics." That's why the CERIAS (pronounced "serious") takes a multidisciplinary approach to information protection.

With nearly 20 faculty members from eight Purdue departments and the aim to work with researchers in industry, government, and other academic institutions worldwide, CERIAS is devoted to tackling areas of information security and assurance from various perspectives, including-

- Computer and network security
- Communications security
- Public policy regarding information security
- Information management and policy development
- Social, legal, and ethical aspects of information use and abuse
- Economics of information assurance
- Electronic commerce security
- Risk management for computing systems and networks
- Awareness and training methods for INFOSEC professionals
- Computer crime investigation and response
- Information warfare issues.

The center, which was founded in May 1998, leverages the strengths of Purdue's Computer Operations, Audit, and Security Technology (COAST) laboratory.

Spafford established the COAST laboratory in 1992 to meet the growing need for research and education in the information security arena. Since then, the COAST laboratory has designed and developed many widely used tools and education materials in computer security, operations systems, and software engineering. Government agencies, businesses, and academic institutions worldwide have hailed these products as models for their usefulness. Today, the COAST works as a partner with the newly established center. Because of its association with CERIAS, COAST is now one of the largest academic computer research groups in the world. Additionally, many of the CS-specific laboratory efforts of COAST have become CERIAS efforts, providing these existing efforts with access to a greater resource base than before.

"Information security is the combination of computer security and communications security, unfortunately little educational infrastructure exists for training people to deal with these issues and none take a broad view of the problems involved," states Spafford.

In addition to its inclusion of COAST resources and faculty, the CERIAS-given its center status-can leverage resources and staff from any department or school. According to Spafford, "No other place in the world is taking the big picture that we do."

CERIAS, given its broad resources and the established reputation of COAST, has already attracted professors and students from 13 countries. In addition, 40 percent of the students are female. The diversity of the faculty and students in CERIAS is reflected in its numerous ongoing COAST research topics, which span from intrusion detection, firewall and software evaluation, authentication, and security archive to vulnerabilities database and testing. The following paragraphs describe some of these efforts.

DEVELOPING A DIFFERENT APPROACH TO INTRUSION DETECTION

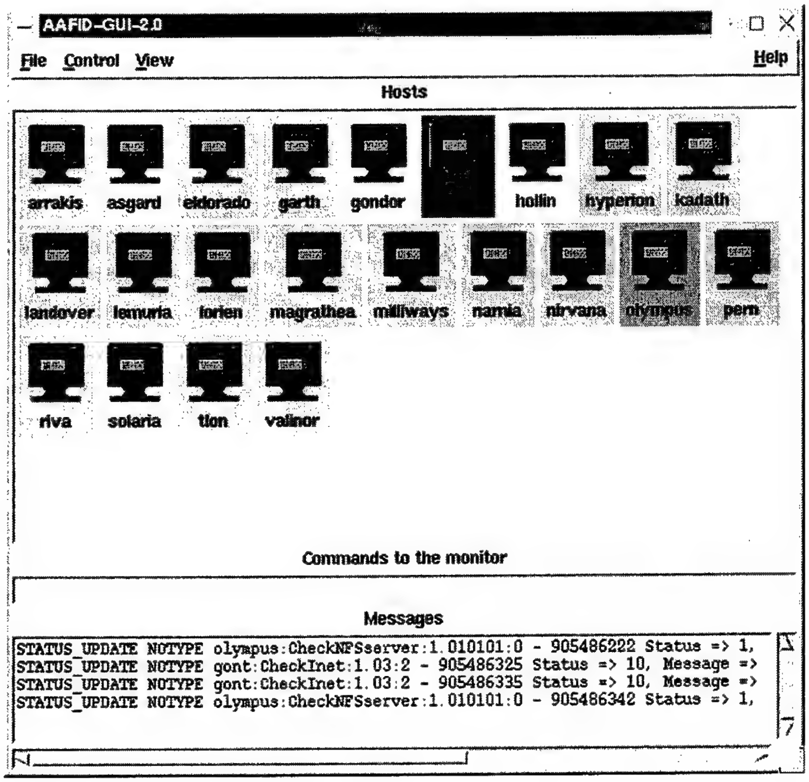
Intrusion detection (ID) is a field within computer security that has grown rapidly during the last few years. The AAFID (Autonomous Agents for Intrusion Detection) project focuses on improving ID methods.

Traditional intrusion detection systems (IDS) collect data from one or more hosts and process the data in a central machine to detect anomalous behavior. This approach, however, prevents scaling of the IDS to a large number of machines because of the storage and processing limitations of the host that performs the analysis.

The AAFID architecture uses many independent entities called "autonomous agents," which work simultaneously to perform distributed ID. Each agent monitors certain aspects of a system and reports anomalous behavior or occurrences of specific events. For example, one agent may search for incorrect permissions on system files, another agent may search for improper configurations of a FTP server, and yet another may search for attempts to perform attacks by corrupting the ARP (Address Resolution Protocol) cache of the machine.

The results the agents produce are collected on a per-machine level, permitting the correlation of events reported by different agents that may be caused by the same attack. Furthermore, reports produced by each machine are aggregated at a higher (per-network) level, allowing the system to detect attacks involving multiple machines.

The AAFID group consists of 10 graduate and undergraduate students within the COAST laboratory. They released a prototype implementation that can be found at the AAFID project web page at http://www.cs.purdue.edu/coast/projects/autonomous-agents.html/.



```
STATUS_UPDATE NOTYPE olympus:CheckNFSserver:1.010101:0 - 905486222 Status => 1,
STATUS_UPDATE NOTYPE gont:CheckInet:1.03:2 - 905486325 Status => 10, Message =>
STATUS_UPDATE NOTYPE gont:CheckInet:1.03:2 - 905486335 Status => 10, Message =>
STATUS_UPDATE NOTYPE olympus:CheckNFSserver:1.010101:0 - 905486342 Status => 1,
```

Tripwire®

One of COAST's better known projects is Tripwire®. It was primarily a project of Gene Kim and Professor Spafford. The product is now the most widely deployed intrusion detection security tool worldwide. Tripwire® is an integrity monitor tool for Linux and Unix systems. It uses message digest algorithms to detect tampering with file contents, as might be caused by an intruder virus. In December 1997 Visual Computing Corporation™ obtained an exclusive license from Purdue University to develop and market new versions of the product. For more information visit http://www.tripwiresecurity.com/.

Underfire

Underfire is an ongoing project started in 1997. The Underfire team consists of seven COAST students. The purpose of the team's efforts is to gain direct experience in installing, evaluating, configuring, and using different firewall systems, to investigate new technologies for network perimeter defenses, including next-generation networks such as ATM, and to investigate the integration of host- and network-based security mechanisms with network perimeter defenses. The Underfire team's goal is to create an architecture for automated firewall testing. The final product will be an engine that will test a firewall without human interaction. This will be achieved with a modular system composed of an engine, a packet sniffer, and scripted attacks. The engine will execute the attacks and use the packet sniffer, or other networking protocols, to test the success or failure of the attack. Finally, a report may be generated automatically that will explain the weak points of the firewall based on the attack data.

The Underfire team, having finished its design and initial implementation of the engine, is scripting known attacks. The automatic report generator will need to be completed in the future. Until now, Underfire has taken only protocol-level attacks into account; a future step will be to extend testing to the application level such as RPC and X11. For more information see http://www.cs.purdue.edu/coast/projects/firewalls.html

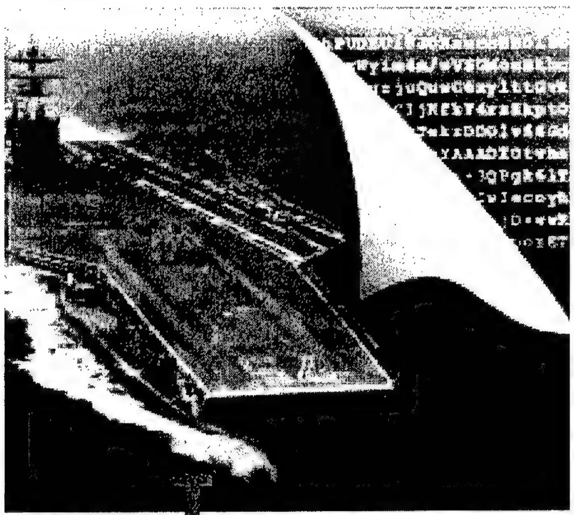
Achieving Next Generation Authentication

Using biometrics devices and tokens such as smart cards and iButtons, several research and application development projects are being conducted in the COAST laboratory to develop ways to authenticate users to systems. The first method is to standardize a common programming interface utilizing on a PC/SC-compliant smart card resource manager written in C++ and cryptographic libraries based on the Public Key Cryptography Standards (PKCS-11 and PKCS-15) specifications. The resource manager allows secure remote authentication by using secure channels to communicate between multiple resource managers. The resource manager will be used to develop many applications including secure login, ssh, xlock, ftp, telnet, etc. using pluggable authentication modules (PAM) along with smart card security. Additionally, students are in-

IATAC chat

by Robert P. Thompson
Director, IATAC

Providing New IA Support to the Warfighter



To support emerging warfighter Information Assurance (IA) needs, IATAC has initiated efforts to create two technical reports supporting critical information assurance (IA) technologies—a state-of-the-art report (SOAR) on Data Embedding for Information Assurance and a critical review and technology assessment (CR/TA) report on Computer Forensics—Tools and Methodology. Each report aims to provide the warfighter with a broader understanding of its subject matter, enabling the warfighter to apply that knowledge when executing his or her IA roles and responsibilities. The following paragraphs briefly describe each report.

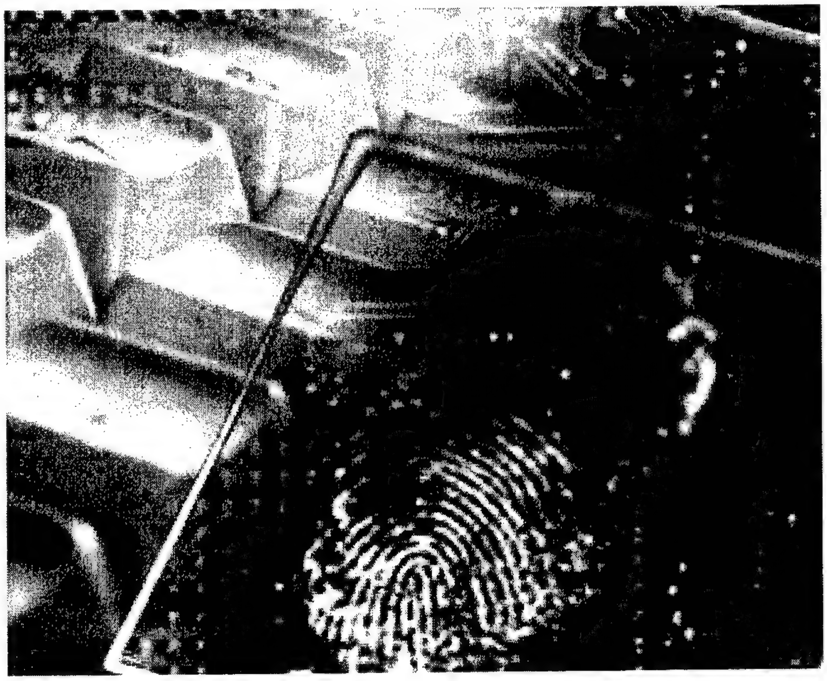
DATA EMBEDDING FOR INFORMATION ASSURANCE

This SOAR introduces data embedding, assesses the state-of-the-art technologies in various data embedding applications, and examines the IA applications of data embedding technologies. The introduction to data embedding reviews relevantterminology, offers a historical perspective of steganography and digital watermarking, and describes in detail the types and uses of data embedding. A state-of-the-art assessment is provided for the following applications: steganography and covert communications, information protection, intellectual property protection, and defenses and attacks. The report examines IA applications of data embedding such as technologies and applications that may pose a specific threat, have an offensive application, and those that may be used for defenseive measures.

COMPUTER FORENSICS—TOOLS AND METHODOLOGY

This CR/TA report introduces computer forensics, protocols and procedures, and forensic tools. The introduction to computer forensics examines legal requirements and reviews traditional computer crimes (e.g., crimes of commerce, violence) and new crimes (e.g., telecommunications fraud, computer intrusion). Protocols and Procedures details the computer forensic process, including acquisition issues, examination variants, and examination output utilization. Commercial-off-the-shelf (COTS) and government-off-the-shelf (GOTS) forensic tools are assessed regarding their ability to support evidence preservation and collection activities. The report also identifies analysis tools that support data recovery, pattern and string matching, and file and file type identification.

The SOAR on Data Embedding for Information Assurance and CR/TA report on Computer Forensics—Tools and Methodology are scheduled for release in March 1999. For more information on available technical reports, contact IATAC at (703) 902-3177 or via e-mail at iatac@dtic.mil.



by William Wall
Harris Corporation

Exactly How Secure is Your WindowsNT™ Computer?

A new security tool available from Harris Corporation's Electronic Systems Sector (Harris) may help users detect, analyze, and correct known security vulnerabilities associated with the Microsoft Windows NT operating system.

The Security Test and Analysis Tool (STAT) uses a database of more than 350 NT vulnerabilities that have been verified and tested in Harris software laboratories to identify existing vulnerabilities in a user's NT network. With STAT, users can assess vulnerabilities in a single computer, multiple computers, or an entire domain. Additionally, via an annual subscription service available from Harris, users can electronically update the STAT database as new security vulnerabilities are identified, patches are released, and enhancements to the functionality of the tool are made.

How STAT works

STAT automatically installs itself on a server or workstation and queries the network to determine which domains and hosts are present. Users then choose whether to operate STAT across single or multiple domains. STAT then identifies nodes by name, address, and operating system. After the domain has been identified, the program can access either individual hosts or the entire domain for security vulnerabilities. The default configuration tests for all vulnerabilities currently available in the STAT database, however, configuration files allow users to select specific vulnerabilities that they would either like to test or ignore for a particular assessment.

When the test is complete and vulnerabilities have been detected, an analysis detailing the security vulnerabilities is provided. The analysis includes the name of the identified vulnerability and its description and risk level. The analysis also offers a solution to correct the vulnerability and links to related web sites and Microsoft knowledge base articles. Fixes can be implemented manually or by an auto-fix feature. After a fix is implemented for a particular vulnerability, users can immediately retest that vulnerability to ensure the fix was successful. STAT also lets users compare previous and current assessments to identify any changes that may have occurred.

Following the analysis, a report of the domain and host status can either be printed, or exported and saved as a text file that can be viewed with any text viewer. Users can format the reports to include selected hosts or entire domains. Users can also customize these reports to create a view of the network's status that is appropriate for executives, supervisors, or technicians.

For more information, visit our website at http://www.STATonline.com for a product overview. This web site also features a security article of the week, frequently asked questions, and links to other computer security sites.

Bill Wall is a senior computer security engineer at Harris. He received his B.S. in Physics from Lenoir Rhyne and his B.S.E.E. from the Air Force Institute of Technology. He is a retired Air Force Officer and has been a computer security analyst for the Air Force and NASA.

The New Arms Race...

Continued from page 8

Next year another DEFCON convention will be held and still more new "weapons" will be released. Although the outcome of our information age arms race is yet to be determined, vigilant and relentless application of the defensive measures described in this article will go a long way toward thwarting malicious attacks. Continued research and development of new technologies, such as VPN and PKI, also promise significant protection in the near future. In the end, however, all these modern technologies are still based on denial of human access to the control pathways of a computer network-once again reinforcing how Strowger's concept from 100 years ago remains our best defense today.

ENDNOTES

[1]Freeman, Roger L., *Telecommuni-cation System Engineering*, 3rd Ed., John Wiley & Sons, Inc., 1996, p. 101.

[2]Meinel, Carolyn P., "How Hackers Break In...and How They Are Caught," *Scientific American*, October 1998, pp. 98-105. This edition provides a number of excellent articles on Network Security to include new defensive tools being implemented and in development. See pages 98 - 117.

[3]Interview with Mr. Phil Loranger, GS-14, Chief, C2 Protect Division, Office of the Director of Information Systems for Command, Control, Communications and Computers, Headquarters, Depart-ment of the Army, 107 Army Pentagon, Washington, DC, 20310-0107., 30 November 1998. Mr. Loranger was a government participant at DEFCON 6.0.

Mr. Loranger is the Army DISC4 Command and Control Protect division chief for the development of the Army's Command and Control Protection program. He received his B.S. in Business Administration and Management from University of Maryland a Master of Technology with a concentration in Information Security from Eastern Michigan University.

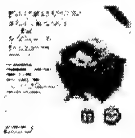
Colonel Mike Brown is the Director of the Information Assurance Office of Director of Information Systems for Command, Control, Communications and Computers (DISC4).

Colonel John Deal is the Executive Officer for the Director of Information Systems for Command, Control, Communications and Computers (DISC4).

continued from page 9

formation across telecommunications systems. Another module discusses transportation modes for information flow via local area networks (LANs), metropolitan area networks (MANs), and wide area networks (WANs). Finally, a module on information flow discusses tools for managing network resources. Examples and real life analogies are given throughout the presentation. The Resources section contains several web sites to learn more about topics discussed in this CD-ROM.

Information Assurance (IA) for Auditors & Evaluators



This interactive CD-ROM begins by identifying, categorizing, and detailing examples of computer crime. Topics of IA covered include threats; countermeasures; confidentiality, integrity, and availability; risk and risk management; and the advantages/vulnerabilities of networked systems. Laws and directives related to IA are also discussed. Overviews of certification & accreditation and the DITSCAP are encapsulated in one module. Additionally, there is a module on reliability risk, data testing (general controls, application controls, access controls), reporting on evidence, and key steps in assessing reliability. Finally, there is an in-depth, interactive practical exercise that allows the user to assess reliability risk, examine system controls, and determine the degree of data testing required. The user will use information presented in a fictional animated film to follow the audit trail of a rogue's missile purchases, using techniques learned in this CD-ROM. A glossary and resources section is included in this product.

FORTEZZA Installers Course for W indows NT

This interactive CD-ROM is designed to provide installers with a basic level of instruction needed to install card readers, card drivers, and FORTEZZA-enabled applications on PCs running Windows NT. Topics covered include concepts of PC card technology, including PC card hosts and sockets, mechanical/electrical aspects and software, and PC card use and compatibility. The installation of PC card readers and drivers is also covered. The user will learn about FORTEZZA installers concepts (security algorithms, security services, encryption, and certificates) as well as FORTEZZA applications, such as MS ArmorMail and AT&T Secret Agent. The final lesson is a diagnostics and troubleshooting session that allows the user to practice problem resolution.

VIDEOS

Networks at Risk

A 10-minute video produced by NCS that deals with hackers, network intrusion, and computer security in the workplace. Topics covered include the selling of electronic information, prevention of network intrusions, password protection, and the importance of auditing network security.

Protect Your AIS

A 15-minute video containing six INFOSEC-related dramatizations of security concerns in the workplace. These sketches demonstrate the need for password protection, virus prevention, user ID security, and controlled access to computer equipment.

The Information Fr ontline

A 10-minute video on Defensive Information Warfare (IW-D) awareness that demonstrates how information is easy to exchange but difficult to protect, the types of IW threats that exist, and the vulnerabilities of information systems. Also describes intelligence agencies that perform IW-D functions.

Bringing Down the House

A 10-minute video describing various hacker intrusions and how they relate to Information Warfare. The main portion of the video covers how hackers use the information superhighway to access systems.

Computer Security 101 (DOJ)

John Walsh of America's Most Wanted hosts this 11-minute video about safeguarding computer information. Three aspects of computer security are discussed: sensitive information (what kind of information needs to be protected), risk management (reasons why computer security is important), and accountability (assuming responsibility for protecting one's computer).

Computer Security, The Executive Role (DOJ)

This 9-minute video stresses the need to protect information systems at all levels of government. The user should be aware that the Office of Management and Budget (OMB) has classified all federal information as "sensitive." To this end, steps to secure workspaces and protect data are delineated. Topics covered include the Computer Security Act of 1987, types of threats to information systems, and risk management.

Understanding PKI (DOD)

This 13-minute video introduces the concept of Public Key Infrastructure (PKI) and how it can be used to ensure the security and privacy of cyber-based transactions. Topics covered include examples of how PKI works, why it is necessary to protect the Defense Information Infrastructure (DII) and National Information Infrastructure (NII), and how it ensures the confidentiality, integrity, non-repudiation, and authentication of electronic messages through digital signatures.

Exploring MISSI

This 10-minute video describes NSA's framework for systems security across the Defense Information Infrastructure (DII) and the National Information Infrastructure (NII). Steps that have been taken to ensure the integrity and safety of information are discussed.

DOD INFOSEC Training and Awareness Products

Order Form

INFOSEC Program Management Office
5111 Leesburg Pike, Suite 100
Falls Church VA 22041-3206
Attn: Product Distribution

Commercial: 703-681-7944/1344 *DSN:* 761-7944
Fax: 703-681-1386
E-mail: DODIAETA@ncr.disa.mil
Homepage: http://www.disa.mil/infosec

How did you hear about our products?

○ DISSPatch ○ WWW ○ Word of Mouth
○ *Conference ○ *Class ○ *Other
*Specify ______________________

Mailing Information

Name ______________________ Title __________ Date ________ WWW Access: ○

Command/Org/Agency ______________________ Dept/Mail Code ____ Phone __________ DSN ____

Address ______________________________ Fax ______________

City ______________ State ____ Zip+4 __________ E-Mail ______________

Mark appropriate organization:

○ CINC/Joint Staff ○ Army ○ Navy ○ AF ○ Marines ○ OSD
○ Defense Agency (name) ______________ ○ Non-Defense Agency (name) ______________
○ Contractor (Agency contracting with) ______________ ○ Other ______________

Order Form

Products are unclassified and available at no cost. Products, excluding CD-ROMs, may be reproduced (for government use only) without further permission.

Multimedia CD-ROMs

○ **DOD or... ○ Federal INFOSEC Awareness, V.1 (Select One)**
○ **DOD INFOWAR Basics, V.1**
○ **Operational Information Systems Security (OISS), Vol. 1, V.1.1**
Operational Information Systems Security (OISS), Vol. 2, V.1
○ **Fortezza Installers Course for Windows NT 4.0, V.1** NEW!
○ **Introduction to the DITSCAP, V.1** NEW!
○ **Information Age Technology, V.1.03** NEW!
○ **IA for Auditors and Evaluators, V.1.04** NEW!

Videos

○ **Networks at Risk (NCS)** *(10 min)*
Protect Your AIS (US Govt) *(6 vignettes)*
Information Front Line (IW)(IC) *(10 min)*
Bringing Down the House (IW)(NSA) *(11 min)*

Videos continued

○ **Computer Security 101 (DOJ)** *(10:58 min)*
Computer Security - The Executive Role (DOJ) *(9 min)*
○ **Exploring MISSI (DISA/NSA)** *(10 min)*
○ **Understanding PKI (DOD)** *(13 min)* NEW!

UPCOMING PRODUCTS

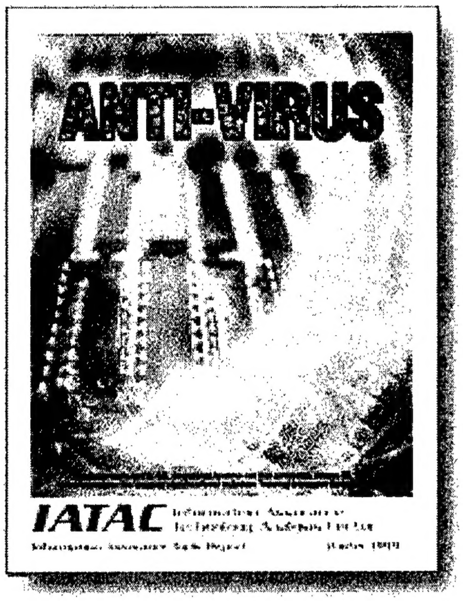
Multimedia CD-ROMs

Designated Approving Authority Basics (DAA), V.1

DISSPatch - DOD INFOSEC Newsletter

○ Add to Mailing List ○ Remove from Mailing List
○ Address Change

What's New


ANTI-VIRUS
IATAC Information Assurance Technology Analysis Center
Information Assurance Tools Report
Winter 1999

IA Anti-Virus Tools report now available to registered DTIC users!

The report provides an index of anti-virus tools that are contained in the IATAC IA Tools database. Each entry provides an overview of the product, as well as, contact information.

Research for this report entailed reviewing various journals and open source data. A total of 60 tools were identified and are currently available in the commercial marketplace. The products listed have all been tested on various platforms, to include, DOS, Windows, Windows 95, Windows 98, Windows NT Workstation, Windows NT Server, OS/2 Warp and Netware.

For instructions on obtaining a copy of the report, refer to the IATAC Product Order Form, opposite on page 21.

COMING IN MARCH

Data Embedding for
Information Assurance
Computer Forensics—
Tools and Methodology

Other Products

Vulnerability Analysis Tools Report

This report provides an index of vulnerability analysis tool descriptions contained in the IA Tools database. It summarizes pertinent information, providing users with a brief description of available tools and contact information. It currently contains descriptions of 35 tools that can be used to support vulnerability and risk assessment.

Modeling & Simulation Technical Report

This report describes the models, simulations and tools being used or developed by selected organizations that are chartered with the IA mission. Data collection efforts focused on the current definitions of Information Operations, Information Warfare, and IA as described in DoD Directives S-3600.1, "*Information Operations,*" and Chairman, Joint Chiefs of Staff Instruction 6510.1A, "*Defensive Information Warfare Policy.*" In addition, the definitions prescribed by DMSO for model and simulation were used to determine what entities should be included in this IA models, simulations and tools report.

Intrusion Detection Report

This report provides an index of intrusion detection tool descriptions contained in the IATAC IA Tools Database. Information was obtained via open source methods, including direct interface with various agencies, organizations, and vendors. Research for this report identified 43 intrusion detection tools currently employed and available.

Malicious Code Detection State-of-the-Art Report (SOAR)

This SOAR includes a taxonomy for malicious software to provide the audience with a better understanding of commercial malicious software. An overview of the current state-of-the-art commercial products and initiatives, as well as future trends is presented. The same is then done for current state-of-the-art in regards to DoD. Lastly, the report presents observations and assertions to support the DoD as it grapples with this problem entering the 21st century. This report is classified and has a limited release.

Product Order Form

IMPORTANT NOTE: *All IATAC Products are distributed through the Defense Technical Information Center (DTIC). If you are NOT a registered DTIC user, you must do so PRIOR to ordering any IATAC products. To register with DTIC go to http://www.dtic.mil/dtic/regprocess.html.*

Name ____

Organization ____________________________ Ofc. Symbol ____________

Address ____________________________ Phone ____________________

____________________________ E-mail ____________________

____________________________ Fax ____________________

____

DoD Organization? □ YES □ NO If NO, complete **LIMITED DISTRIBUTION** section below.

LIMITED DISTRIBUTION	**QTY.**	**PRICE EA.**	**EXTD. PRICE**

In order for NON-DoD organizations to obtain LIMITED DISTRIBUTION products, a formal written request must be sent to IAC Program Office, ATTN: Sherry Davis, 8725 John Kingman Road, Suite 0944, Ft. Belvoir, VA 22060-6218

Contract No. ____

For contractors to obtain reports, request must support a program & be verified with COTR

COTR ____________________________ Phone ____________________

□ **Modeling & Simulation Technical Report**		No Cost	
□ **IA Tools Report — Firewalls**		No Cost	
□ **IA Tools Report — Intrusion Detection**		No Cost	
□ **IA Tools Report — Vulnerability Analysis**		No Cost	
□ **Malicious Code Detection SOAR** □ TOP SECRET □ SECRET		No Cost	

Security POC ____________________________ Security Phone ____________________

UNLIMITED DISTRIBUTION	**QTY.**	**PRICE EA.**	**EXTD. PRICE**
□ **Newsletters** *(Limited number of back issues available)*			
□ Vol. 1, No. 1 □ Vol. 1 No. 2 □ Vol. 1 No. 3 □ Vol. 2, No. 1 □ Vol. 2 No. 2 □ Vol. 2 No. 3		No Cost	
		ORDER TOTAL	

Please list the Government Program(s)/Project(s) that the product(s) will be used to support: ____________________

____

____

Once completed, Fax to IATAC at 703.902.3425

Calendar

FEB 9-13

Intrusion Detection & Response
San Diego, CA
Features in-depth courses taught by SANS faculty.
call 301.951.0102
www.sans.org/id/call.htm

MAR 2-4

Southeast Command, Control, Communications, Computers & Intelligence Conference and Exposition
Tampa, FL
Sponsored by the AFCEA Tampa-St. Petersburg Chapter
call J. Spargo & Associates Inc., 703.631.6200
www.jspargo.com/events.htm

MAR 9-11

Fourth Warfighter Information Assurance Symposium
Kossiakoff Center, Johns Hopkins University, Laurel, MD
Sponsored by the National Security Agency, Information Systems Security Organization
call 410.850.7156
warfighter@mcneiltechmd.com

MAR 15-17

InfoSec World: Open Systems Security '99 and ISSA Annual Conference
Orlando, FL
Topics include intrusion detection, single sign-on, smart card security and hacker tools and trends.
www.misti.com

APR 18-21

Association of Old Crows (AOC) FIESTACROW '99
San Antonio, TX
Sponsored by the Billy Mitchell Chapter, AOC and cosponsored by AFCEA Alamo Chapter
call 210.732.7697
www.fiestacrow.org

MAY 9-15

SANS99: 8th International Conference on System Administration, Networking and Security
Baltimore, MD
Covers networking, security and intrusion detection.
www.sans.org

We've Moved

3190 Fairview Park Drive
Falls Church, VA 22042

Phone	703.289.5454
Fax	703.289.5462
STU-III	703.289.5467
E-mail:	iatac@dtic.mil
URL:	www.iatac.dtic.mil

Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church, VA 22042